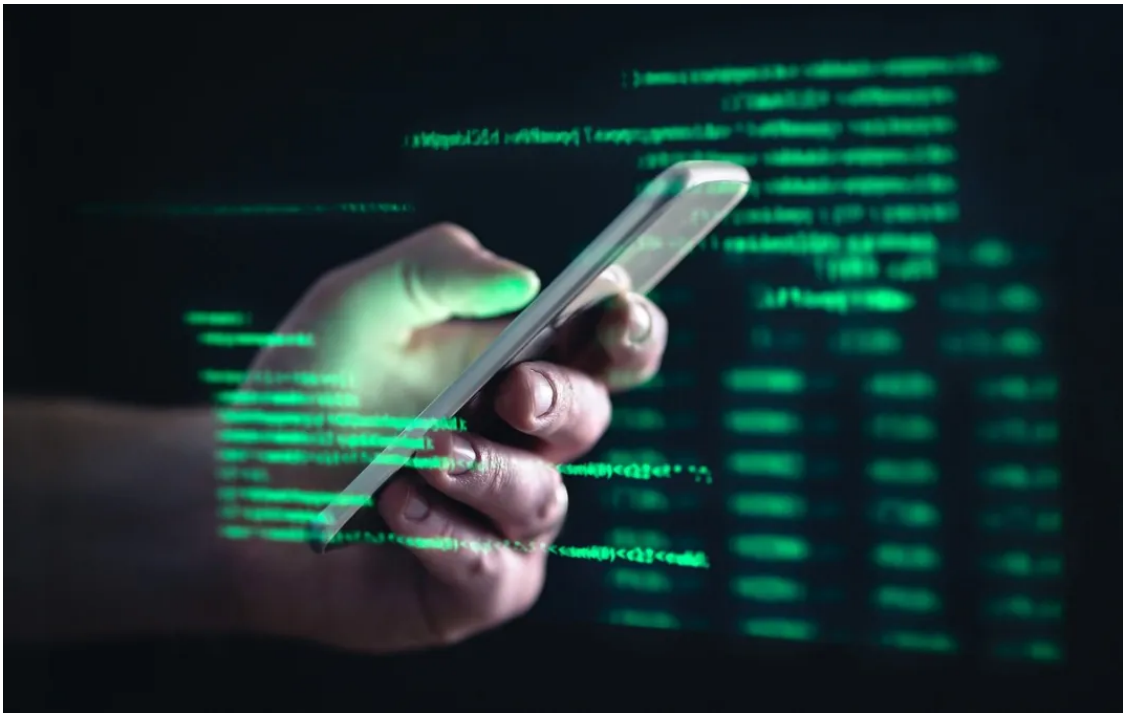
Como seus dados são rastreados na internet

By **Gabriel Camargo** 04/10/2022



Créditos da imagem: Olhar Digital

O artigo dessa semana foi amplamente baseado no último capítulo de meu livro “Moldados pelo poder: uma perspectiva libertária da história mundial”, ainda em processo de escrita. No segundo artigo da série, analisarei as capacidades dos diferentes adversários encontrados no mundo digital.

Agentes mal-intencionados

Não é costume se proteger daqueles que estão mais perto. Por convivência, por vezes, todos os dias, são encarados como presença normal. Com o hábito, vem a confiança. Com a confiança, vem o descuido. Por estarem próximas, essas pessoas têm acesso privilegiado a informações. Ainda, com a união do que sabem no mundo físico com o que têm acesso no mundo digital, pessoas próximas mal-intencionadas podem se tornar ameaças significativas.

Para a segurança, caso haja disputas legais, interesses financeiros ou competição para uma vaga de emprego, desde compartilhamento de cartões de crédito até disputas por heranças, adversários bem informados podem utilizar do que possuem para tentar ganhar vantagem ao prejudicar o outro.

Sobre a privacidade, amigos podem compartilhar informações que não eram para se tornar públicas. Antigos parceiros podem tentar danificar ou mesmo destruir reputações. Em um mundo como o atual, a internet dificilmente esquece. Danos sofridos por exposições ou acusações indevidas podem danificar a vida futura, dificultando desde o encontro de novos parceiros(as) até a empregabilidade e confiança depositadas.

Colegas de trabalho podem ter interesse sexual por alguém que não os corresponda. Cuidados relativos aos dados e informações disponíveis (como no caso do compartilhamento de informações em redes sociais, incluindo localizações e locais frequentados) podem auxiliar na mitigação de problemas futuros.

Informações publicamente disponíveis podem ser utilizadas no planejamento de ataques. Informações relativas a uma viagem ou à escola onde os filhos estudam podem ser utilizadas para esse propósito. Minimizar o compartilhamento de informações reduz a superfície de ameaça.

Anúncios digitais e o rastreio de dados na web

Caso as informações pertencentes ao público geral fossem irrelevantes, por qual motivo as empresas e agências governamentais gastariam bilhões de dólares no rastreamento dos usuários? Claramente há incentivos. Ainda, para alguns adversários, não é nem mesmo necessário um motivo para a coleta; eles a fazem porque podem.

A maioria dos sites monitora o comportamento de seus visitantes. As técnicas de rastreamento estão sempre avançando. Novas tecnologias, como o JavaScript e o HTML5, possibilitaram novas maneiras de obtenção de dados dos usuários.

Iniciando por uma tecnologia mais antiga, os cookies são pequenos arquivos armazenados no dispositivo do usuário, com informações relevantes para a navegação. Alguns cookies são úteis ao usuário, como aqueles que guardam as preferências dos sites que são visitados com frequência ou os que guardam dados dos produtos no carrinho, quando são efetuadas compras online. A adição dos produtos não precisa ser constante, pois as informações da sessão estão armazenadas no cookie.

Alguns cookies, por outro lado, são úteis aos anunciantes. Por si só, também nada de errado. O problema surge por causa da falta de transparência do processo (com a maioria dos usuários desconhecendo as práticas

adotadas), da quantidade de informações coletadas (podendo ser suficientes para traçar um perfil avançado de interesses), do armazenamento de informações coletadas por tempo desconhecido (por vezes, indeterminado) e do compartilhamento das informações coletadas com terceiros diversos, nem sempre bem-intencionados.

Pode-se dividir os cookies em first-party (mesma origem) ou third-party (de terceiros). Os cookies de mesma origem podem ser persistentes ou efêmeros. Apresentam menor ameaça à privacidade, mas podem ser utilizados para rastreio e construção de perfis. Como o nome indica, são utilizados apenas pelo site de origem. Os cookies de terceiros podem também ser persistentes ou efêmeros. Acessados por sites que não os criaram, aumentam a capacidade de rastreamento frente aos de mesma origem. A transmissão das informações armazenadas no cookie não necessita de interação do usuário, bastando o site, com conteúdo de anunciantes e/ou de redes sociais, ser carregado.

Beacons são rastreadores presentes em páginas web, anúncios e mensagens de e-mail, capazes de capturar informações como o horário relacionada à abertura do e-mail e o endereço IP da conexão. Comumente associados aos cookies, geralmente consistem de pequenas imagens ocultas e/ou de 1×1 píxel. Têm capacidade de se conectar a servidores de terceiros, que implantam cookies no navegador do usuário. Esse cookie é reenviado ao servidor quando o usuário navega para outro site que também contenha beacons do mesmo serviço, o que, ao longo do tempo, pode criar um perfil contendo uma grande proporção dos hábitos de navegação. Beacons também são utilizados para verificar a existência de cookies já armazenados, sendo também capazes de enviar informações adicionais, como o tipo de navegador e dispositivo utilizado.

Anunciantes e empresas utilizam parâmetros nos endereços web para a coleta de informações acerca do grau de sucesso de seus anúncios. Ainda, esse tipo de rastreamento pode ocorrer quando um website adiciona identificadores únicos às URLs antes do usuário deixar o site. Scripts nos sites de destino podem, então, ler o identificador, obtendo conhecimento sobre parte da navegação efetuada.

Os endereços IP (internet protocol) são comumente utilizados para o rastreamento na internet. Por meio dessa informação, pode-se revelar a localização física aproximada do usuário, revelar as atividades peer-to-peer (P2P) vinculadas ao endereço em questão (possível pela utilização de infraestrutura monitorada), bem como rastrear fragmentos em servidores web diversos, possivelmente construindo um perfil de navegação e

identificação.

Ao contrário dos endereços IPv4, comumente situados atrás de um roteador com NAT, em outras palavras, uma espécie de firewall, endereços IPv6 normalmente conectam dispositivos diretamente à internet, com a consequente perda de proteção proporcionada pelo NAT. As atividades de um usuário são individualizadas, não mais se beneficiando do pool gerado pelo compartilhamento de IP, devido a um roteador em IPv4.

Todas essas informações obtidas podem ser compartilhadas entre as diferentes empresas, possibilitando a criação de um perfil significativamente aprofundado sobre cada usuário da rede. A segurança na armazenagem desses dados, que vão desde sites acessados ao histórico de localização, é comumente deficitária, ficando o usuário exposto caso as empresas sofram ataques ou decidam utilizar os dados coletados de forma questionável.

Métodos mais modernos de rastreamento dependem de uma variada gama de informações e configurações presentes nos navegadores atuais ou acessíveis através deles. Cada site acessado é capaz de identificar diversos parâmetros associados ao navegador e ao dispositivo utilizado, primordialmente, pelo uso de JavaScript. Essas informações compreendem: user agent, idioma, extensões instaladas, tipo/modelo de dispositivo, sistema operacional, lista de fontes utilizadas/instaladas, presença de um bloqueador de anúncios, resolução de tela, hora do sistema, elemento canvas, estado do JavaScript (se habilitado ou não), presença de câmera e microfone, estado da bateria, informações do driver gráfico e arquitetura da cpu. Somadas, essas informações são mais que suficientes para identificar um usuário com precisão, podendo identificar sua navegação por inteiro.

A impressão digital derivada do elemento canvas ocorre quando o usuário navega para uma página com essa funcionalidade de rastreio. Os scripts no site visitado instruem o navegador a gerar uma imagem oculta e, como cada navegador e cada dispositivo interagem de forma ligeiramente diferente com os conteúdos na web, pode-se derivar um identificador próprio.

Quando um usuário acessa uma página, os espaços para publicidade são leiloados algoritmicamente. As informações coletadas para compor o perfil são compartilhadas com as milhares de empresas anunciantes que, por meio do leilão digital, concorrem entre si pelo espaço destinado a ser visto por aquele determinado usuário. Os vencedores ganham o direito de mostrar seus anúncios. Esse processo leva apenas milissegundos. A maior

empresa atuante nesse ramo é a Google, que faz o papel de leiloeiro.

A vigilância das Big Techs

Todo o exposto acima também vale para as gigantes da tecnologia, como Google, Amazon e Meta, por serem os ganhos provenientes dos anúncios uma parte significativa de suas receitas. Seu escopo não se limita a isso, no entanto.

A utilização de sistemas operacionais proprietário, como o Microsoft Windows, abre possibilidades totais de vigilância sobre o que é feito durante seu uso. Sabe-se que, como esse tipo de sistema pode ser considerado um spyware, algumas de suas capacidades são saber quais aplicativos foram abertos e o tempo gasto em cada um deles, mas, em teoria, todas as ações realizadas poderiam ser vigiadas, logadas e enviadas aos servidores da empresa.

A localização de um usuário, para a sua privacidade, é uma das informações mais importantes disponíveis. Adicionalmente à criação de um mapa 3D das ruas e cidades, projetos como o Google Street View tinham propósitos pouco conhecidos pelo público geral. Um deles era o mapeamento, em nível global, das redes sem fio. Por meio desse mapa global, que associa localização com o endereço MAC do ponto de acesso, empresas como Google e Apple têm a capacidade de saber a localização do usuário por meio das intensidades de sinal de redes próximas, realizando triangulação; a precisão desse método pode chegar a dois metros. Esse método é atualmente realizado pelos celulares, que constantemente varrem as redes sem fio próximas, relacionando suas forças de sinal e a localização associada ao GPS do dispositivo.

Celulares modernos comuns são dispositivos espiões. Com o mapa criado pela Google, a empresa utiliza seu banco de dados para permanentemente rastrear seus usuários. Os celulares modernos enviam constantemente dados de rastreamento e analytics para os servidores das grandes empresas de tecnologia. Essa ação não pode ser desligada. Aparelhos Android conectados ao Google enviam fluxo constante de dados, desde parâmetros de localização até quais aplicativos foram abertos pelo usuário.

Além do rastreamento realizado pelo próprio sistema operacional, todos os aplicativos instalados nos dispositivos podem também coletar dados. É constante a comunicação e o envio de dados entre os dispositivos móveis e servidores de anunciantes e/ou empresas especializadas na criação e venda de perfis de usuários. Como consequência, não há privacidade no uso de

dispositivos móveis modernos sem modificação, e seu uso não é recomendado em determinadas situações, como quando se participa de um protesto.

A Apple também realiza verificações no conteúdo armazenado nos iPhones, supostamente para procurar imagens de pornografia infantil. Essa capacidade, contudo, pode ser facilmente convertida para a procura de qualquer tipo de conteúdo armazenado nos aparelhos, nada impedindo o posterior contato com forças policiais quando um match for estabelecido. Tecnologicamente, a única mudança necessária seria a alteração dos parâmetros de procura.

Apple e Amazon, por meio da tecnologia de bluetooth de baixa energia, construíram uma vasta rede mesh, utilizando iPhones e AirTags (no caso da Apple) e dispositivos Alexa Echo e Ring (no caso da Amazon).

Com a disseminação das AirTags da Apple, todos os iPhones, mesmo os não pertencentes aos donos das AirTags, são integrados na rede mesh. O sistema operacional de todos os novos iPhones procura constantemente por AirTags próximas. Caso detecte o sinal, os dados são enviados para os servidores da empresa, junto à localização do dispositivo que o captou.

O que essa tecnologia proporciona é a correlação de dados para inferir quem estava nas proximidades do usuário. Caso um dono de uma AirTag vá a uma festa e a tenha, por exemplo, em seu molho de chaves, e dez pessoas nessa festa usam iPhones, todos eles enviariam a identificação do sinal para os servidores da Apple, que conseguiria inferir que todos estavam no mesmo lugar naquele momento. No caso, em uma mesma festa.

Com a disseminação desse tipo de tecnologia, que não necessariamente é restrita à Apple, o rastreamento de contatos poderá ser realizado em tempo integral; as Big Techs sempre sabendo quem está na presença de quem. Essa ação não é opcional, portanto, não pode ser desligada.

Com a introdução da internet das coisas, cada novo dispositivo inteligente trará consigo não apenas novas vulnerabilidades e pontos de entrada para as redes das quais fazem parte, mas aumentarão a coleta de dados. As possibilidades são vastas. De imagens 24 horas de câmeras de segurança, equipadas com inteligência artificial, a todas as palavras ditas por uma pessoa em sua residência, no caso de dispositivos como Alexa. Pensar que dispositivos como esse não estão sempre enviando o que veem e escutam para servidores das empresas de tecnologia, é um ato de pura confiança. Capacidade, certamente eles têm.

É comum que fotos tiradas por câmeras digitais tenham metadados embutidos. Caso esses metadados não forem removidos, dados referentes ao modelo de câmera, data, hora e mesmo a localização de onde foi tirada podem ser enviados indiscriminadamente.

Em muitos casos, todos os metadados podem ser acessados, mesmo por usuários que posteriormente façam o download das fotos, após terem sido compartilhadas, por exemplo, em redes sociais. Inteligências artificiais utilizam fotos de redes sociais para o treinamento de seus algoritmos. Todas as fotos enviadas ao Facebook são escaneadas por inteligências artificiais, capazes de reconhecer e classificar identidades.

Todos os e-mails presentes no Gmail podem ser escaneados, ou mesmo lidos por terceiros, para a extração de informações úteis aos anunciantes. Outros serviços de e-mail fazem o mesmo. Ainda, pela própria natureza tecnológica dos e-mails e demora em atualizar os padrões de segurança, muitos ainda viajam pela internet descriptografados. Existem maneiras de proteger o conteúdo, como a utilização de provedores que possibilitem o uso de PGP, mas os e-mails enviados pela internet podem ser interceptados por agências de inteligência e hackers privilegiados. E mesmo criptografando o corpo, os metadados permanecem sem proteção.

Todas as pesquisas no Google são logadas e associadas a um perfil. É possível alterar o que é visto por um usuário e suprimir que certas informações cheguem até ele, com base no perfil traçado pela análise dos dados coletados. Para isso, podem ser usadas técnicas simples, como a alteração da ordem em que as informações aparecem nas páginas de resultados, elevando ou depreciando seletivamente as informações.

Por meio do acesso à lista de contatos do usuário, que pode ser obtida por diferentes formas, bem como o acesso aos metadados das comunicações, é possível estabelecer um mapa de relações, do qual se derivam significativas informações, mesmo quando criptografadas em conteúdo. Criptografia de ponta a ponta não necessariamente protege os metadados.

Com a nova geração de carros inteligentes, bem como a disseminação semiforçada dos carros elétricos e autônomos, a tecnologia embarcada torna os automóveis verdadeiros computadores conectados à internet.

O envio da localização em tempo real (e junto a isso o registro de todas as rotas percorridas) de todos os automóveis modernos já é algo possível. Carros modernos são capazes de armazenar quais rádios você sintonizou. Equipados com câmeras de inteligência artificial, os carros autônomos

possuem capacidade de gravar e compartilhar vídeos de seu interior e entorno, mesmo quando o carro não está em uso.

Com a sincronização de smartphones ao automóvel, informações como identificadores do celular, lista de contatos e registro de chamadas também ficam disponíveis ao fabricante. Tecnologicamente, é possível, por meio da identificação de um usuário de interesse, impedir o uso de seu “próprio” veículo.

De script kiddies a crackers

Comumente associados à segurança, criminosos digitais também proporcionam danos e estragos na privacidade e anonimato dos usuários. Por meio da invasão e venda de dados/informações obtidas, pode-se realizar ataques de roubo de identidade e, de posse dos dados pessoais, atacantes abrem contas em banco ou pegam empréstimos no nome da vítima.

Vazamentos de dados são comuns. Caso dados de login sejam obtidos, os atacantes com frequência os testam em outras plataformas para tentar comprometer mais contas. Como muitos usuários utilizam as mesmas senhas em serviços diferentes, essa prática muitas vezes é bem-sucedida. Um ponto crítico são contas de e-mail, pois comumente agregam comunicações de outros serviços, armazenam grande quantidade de informações passadas e ainda servem de confirmadores no processo de troca de senhas.

Por meio de ataques massificados (ou mesmo diretos), e-mails contendo links que apontam para sites maliciosos podem ser utilizados para comprometer a segurança de seu dispositivo. E-mails com anexos contendo códigos maliciosos também são comuns. Malwares e ameaças como rootkits, backdoors, caválos de tróia e spywares comumente entram em um dispositivo por descuido do usuário. Muitos atacantes não possuem conhecimento necessário para construir seus próprios malwares, sendo possível comprar ou alugar serviços de criminosos mais experientes e com maior nível de conhecimento.

Ataques direcionados geralmente são mais sofisticados. Crackers com habilidades excepcionais, ou que trabalham para governos, lançam campanhas contra um grupo reduzido de indivíduos, como jornalistas em um país autoritário, ou mesmo em um combate digital entre países. Com objetivos diversos, que vão desde pura espionagem e roubo de dados até a destruição física dos dispositivos, esses malwares sofisticados podem passar tempos consideráveis indetectados no sistema de interesse.

Ataques, sofisticados ou não, comumente dependem de descuidos do usuário para obter sucesso, mas nem sempre esse é o caso. Atacantes podem utilizar vulnerabilidades (conhecidas ou não) para adquirir acesso ao sistema. Alguns ataques sofisticados não necessitam da interação dos usuários, sendo automaticamente bem-sucedidos com a simples abertura de um site ou o recebimento de uma mensagem SMS. Ainda, como mensagens de SMS não são criptografadas, podem ser interceptadas por adversários no meio do caminho. Sites legítimos também podem ser comprometidos e utilizados para infectar usuários que de nada suspeitam.

Ataques que utilizam engenharia social exploram a curiosidade, o medo, a empatia e a vontade de ganhar vantagem para enganar as vítimas. Ataques podem ter motivação financeira direta, destrutiva ou de espionagem. Ou mais de um motivo em simultâneo. Em celulares, por exemplo, além de espionar o usuário, custos adicionais podem ser gerados pelo envio de SMS a serviços pagos.

Tendo obtido acesso a um sistema, o atacante pode executar movimentos laterais para comprometer outros equipamentos conectados à mesma rede. Nos dispositivos, pode abrir portas ocultas de comunicação para receber futuras instruções do atacante, bem como copiar dados e informações do sistema atacado. Dependendo do nível de sofisticação e dos objetivos do malware, todas as palavras digitadas poderão ser enviadas ao atacante (com todas as senhas e informações privadas inseridas no teclado).

Câmeras e microfones podem ser ligados sem que a luz indicadora seja acesa. Capturas de tela podem ser realizadas e enviadas para os servidores controlados pelo atacante, ou mesmo o sistema pode ser destruído, incluindo em nível de hardware.

Com a popularização de criptomoedas, os usuários necessitam de maiores cuidados para gerir seus bens e ativos digitais, o que abre portas para novos tipos de ataque. Pode-se tirar vantagem do tamanho reduzido de redes de mineração para a realização de um ataque de 51%, no qual os atacantes obtém o controle da rede e, com isso, podem modificar as transações realizadas.

Métodos avançados de rastreamento de dados

O rastreamento do cursor do mouse ocorre com o uso de JavaScript, CSS, plugins ou softwares específicos. Essa tecnologia de rastreio proporciona a coleta da localização do ponteiro, dos cliques efetuados, do tempo em que

se permanece em determinada área da página, da passagem do mouse por links e a duração dessa passagem, do traçado completo do ponteiro e correlação com o horário da ação.

Esse tipo de tecnologia permite a identificação de usuário previamente considerado anônimo, pois cada usuário possui uma maneira de interagir com o mouse e as páginas web, o que, ao longo do tempo, pode ser utilizado para criar um identificador único.

A identificação de usuários considerados anônimos também pode ocorrer por meio dos padrões de digitação. A velocidade, o tempo que a tecla fica pressionada, erros cometidos, probabilidade de ser destro ou canhoto, abreviações utilizadas, comprimento médio de frases, frequência no uso de palavras, pausas na digitação, dentre outros parâmetros, podem criar uma identidade única, mesmo com a variabilidade natural da escrita ao longo do dia.

Técnicas como essa podem ser utilizadas para identificar um autor de um texto ou documento anônimo, por meio de inteligência artificial e análise estatística.

O Media Access Control (MAC) é um endereço de hardware vinculado às interfaces de rede, como conexões por cabo ou sem fio. Geralmente, um único computador apresenta mais de um endereço MAC, um para cada interface. Dispositivos conectados na mesma rede, ou softwares instalados nesses dispositivos, têm a capacidade de identificar os endereços MAC dos demais dispositivos conectados, proporcionando a identificação de uso de uma determinada rede por um dispositivo em específico.

Ao longo do tempo, e com a correlação de imagens de câmeras de segurança, é possível para um adversário tecnologicamente capacitado identificar as redes às quais o dispositivo se conecta com regularidade e correlacionar com imagens do usuário que realiza essas conexões.

Por meio do ultrassom, novas técnicas de rastreamento estão surgindo no mercado tecnológico. Um cenário possível é a exibição de propagandas, na internet ou televisão, com áudio na frequência ultrassônica, interceptados pelos microfones dos smartphones presentes no ambiente.

Caso aplicativos capazes de interpretar as informações presentes no áudio estejam instalados no aparelho móvel, é possível relacionar os hábitos de consumo de mídia com a identidade do usuário do dispositivo. A utilização de ultrassom também pode revelar as identidades de pessoas próximas ao

usuário, bem como a frequência de interação entre elas.

Na maioria dos navegadores, o histórico e o cache são compartilhados, o que abre margem para ataques de sniffing. Comumente, links visitados são apresentados de formas diferentes dos não visitados. Caso um site com código JavaScript malicioso seja acessado pelo usuário, o atacante pode criar links para sites diversos em regiões ocultas da página, utilizando a interface DOM do navegador para inspecionar a forma na qual os links são apresentados, possibilitando revelar os sites previamente acessados.

Alguns JavaScripts são denominados “session replay”, ou de reprodução de sessão. Com capacidade de armazenar movimentos do ponteiro, rolagem da página, teclas pressionadas, dentre outros; possibilita a completa reprodução da sessão do usuário.

No mundo físico, sua maneira particular de caminhar pode ajudar em sua identificação, mesmo com o uso de máscaras e óculos escuros.

A utilização de informações coletadas pelas forças policiais está sendo utilizada na prevenção de crimes futuros, por probabilidade de cometê-los. Inocentes tornam-se, assim, vítimas de uma inteligência artificial que tenta prever suas ações.

Agências governamentais de inteligência

A NSA foi criada no contexto da Guerra Fria, com o intuito de obter dados de inteligência e proteger informações críticas do governo americano. Para monitorar a União Soviética, por exemplo, instalou grandes antenas em diferentes localidades do globo. Também durante a Guerra Fria, em resposta ao lançamento do satélite soviético Sputnik 1, a DARPA (na época, ARPA) foi fundada para combater os avanços soviéticos e garantir a hegemonia americana.

Para esse fim, além de realizar pesquisas para a criação de tecnologias de uso militar, desenvolveu um sistema de compartilhamento de informações para estimular o avanço científico, criando, em 1969, uma rede de computadores denominada ARPANET, a principal precursora da internet. Já na década de 1970, a ARPANET foi utilizada para auxiliar nos processos de espionagem de ativistas de direitos humanos e antiguerra.

Tendo iniciado com a proposta de conectar poucos computadores, a rede cresceu à medida que seus benefícios tornaram-se claros. A transformação da internet moderna, derivada da anterior rede de uso militar, teve, como

um de seus principais fatores, o seu potencial uso econômico. Após anos de sucessivo crescimento, almejando estender a rede para o mundo civil, o governo americano privatizou sua infraestrutura.

Com a popularização dos computadores de uso individual, além da criação da World Wide Web, nos laboratórios do CERN, a década de 90 foi fundamental para a disseminação da internet. O século XXI iniciou, então, com um mundo em rápido processo de integração digital.

Os ataques de 11 de setembro profundamente abalaram a mentalidade do ocidente, principalmente a americana. Os americanos, por meio de seu patriotismo, sentiram-se individualmente atacados. A opinião pública não tardou a se radicalizar. Medo, raiva, tristeza e vingança; juntamente às demostrações públicas de afeto e união, marcaram o país nos momentos posteriores aos ataques. Esses sentimentos e demonstrações praticamente tornaram-se obrigações.

O estado não desperdiçou essa boa oportunidade e expandiu seus poderes e seu escopo de atuação, com figuras políticas também utilizando o acontecido para enobrecer suas imagens perante o público, que esperava orientação de seus líderes.

Com relação às agências de inteligência, sentindo-se responsáveis por não terem sido capazes de impedir o acontecido, bem como aproveitando a oportunidade que a elas se apresentava, iniciaram uma transformação brutal em suas capacidades e estruturas.

Após os ataques terroristas, as agências cresceram e iniciaram um amplo processo de compartilhamento de informações, bem como realmente decidiram explorar e utilizar as possibilidades proporcionadas pelas ferramentas computacionais. Para isso, contudo, precisavam de novo pessoal: de funcionários imersos na nova geração digital. Um deles foi Edward Snowden, o responsável por, anos mais tarde, divulgar os segredos dos programas de espionagem da NSA, no que foi considerado um dos maiores vazamentos de informações da história da inteligência mundial.

Com a justificativa de combate ao terrorismo e proteção do público, a vigilância não seria mais específica; seria generalizada. Utilizando o poder proporcionado pela nova revolução tecnológica, a inteligência dos Estados Unidos foi capaz de criar um sistema de monitoramento global dos usuários das redes digitais, coletando todo o tráfego que passava em infraestrutura controlada e armazenando as informações coletadas em grandes bancos de dados, ficando à disposição para consulta futura. Todos os sites visitados

por um usuário da internet, todos os e-mails enviados, todas as ligações telefônicas realizadas, todas as buscas feitas, enfim, todas as comunicações alimentam as bases de dados da inteligência dos estados modernos mais desenvolvidos.

Em um mundo cada vez mais digital, uma parte cada vez maior da vida humana encontra-se no virtual. As Big Techs são parceiras estratégicas dos governos participando de projetos e contratos conjuntos. Alguns estados agora tem a capacidade de acessar todo o histórico de um usuário, ao longo de todos os anos de sua vida na internet, utilizando o que encontrar para incriminá-lo ou acusá-lo, mesmo de um crime sem vítimas ou inexistente. Mesmo o que hoje não apresenta problema, no futuro poderá apresentar. Mesmo dados inofensivos tornam-se armas nas mãos de adversários.

O problema pode não estar nos dados em si, mas no uso que é dado a eles; nas possibilidades e no fortalecimento que proporcionam. Como os estados são as entidades criadoras e modificadoras das regras de cumprimento forçado, um histórico completo e permanente torna-se uma poderosa arma contra qualquer indivíduo que não o satisfaça.

Mesmo tendo a capacidade, não é necessário capturar o conteúdo do que está sendo enviado pelas conexões, mas apenas seus metadados (os dados referentes aos dados, como origem e destino), com as agências de inteligência decidindo eliminar indivíduos com base na análise dos metadados de suas comunicações.

Muito do que as agências estatais são capazes de realizar não apenas depende de sua própria infraestrutura, mas da estrutura de vigilância e rastreio adquirida com a parceria (ou invasão) de bancos de dados e servidores das grandes empresas de tecnologia, como Google, Microsoft, Meta e Amazon. As empresas de propriedade particular têm incentivos para rastrear seus usuários para fins econômicos. As agências estatais utilizam dessa estrutura de rastreamento para aumentar sua própria capacidade.

O governo americano, devido à história da internet, encontra-se em uma posição privilegiada (como exemplo, 10 dos 13 servidores raiz de DNS estavam localizados nos Estados Unidos até 2004). Seus principais estados vassalos, como o britânico e alemão, também compondo o processo direto de obtenção e compartilhamento de inteligência. Significativa parte do tráfego mundial passa pelos Estados Unidos ou por equipamentos americanos.

A maior parte dos sistemas operacionais são americanos. A maior parte das

grandes empresas de tecnologia são americanas. Muitos dos maiores fabricantes de hardware e software são americanos. O estado não ignora o poder que obtém. Ele o utiliza para alimentar seus esquemas de perpetuação do poder adquirido. Com a internet, não é diferente.

A coleta também ocorre diretamente nas informações em trânsito, nos provedores de internet e nos cabos submarinos que ligam as diferentes partes da rede mundial. Os dados transmitidos por luz (fibra ótica) são desviados para os servidores de armazenamento das agências de inteligência.

Por meio da análise automática de parâmetros de navegação, as agências também são capazes de flagrar um tráfego de internet encarado como suspeito (os critérios para essa conclusão sendo completamente dependentes das vontades dos agentes), escolher um exploit e enviá-lo junto ao que foi originalmente pedido pelo usuário. O computador comprometido pode, então, ser acessado por completo pelos agentes.

A NSA possui ferramentas para compilar e estruturar os dados provenientes de suas diferentes fontes. Com isso, seus agentes são capazes de pesquisar por qualquer nome, qualquer endereço de e-mail, qualquer número de telefone ou celular e as informações completas sobre o objeto de investigação serão apresentadas. Como em uma pesquisa no Google. O que foi coletado também compreende vídeos e áudios gravados diretamente dos dispositivos dos usuários, os dados obtidos por meio das câmeras e microfones conectados.

A CIA, criada em 1947 para atuar na inteligência externa, utiliza uma variada combinação de técnicas para a penetração e comprometimento de sistemas. Por meio de seu arsenal de armas digitais, utiliza vulnerabilidades desconhecidas para espionagem e destruição de alvos. A CIA é capaz de invadir smart TVs, fazendo-as parecer desligadas, enquanto enviam dados coletados do ambiente para servidores governamentais. São capazes de invadir carros inteligentes e controlar sua trajetória. São capazes de infectar smartphones e interceptar suas comunicações (o que anula a proteção da criptografia utilizada em aplicativos), ligar câmeras e microfones para a captura de dados e rastrear permanentemente a localização do usuário.

As agências de inteligência americana também utilizam consulados como bases secretas de operação no exterior, como no caso do consulado de Frankfurt, na Alemanha, que serve de base para operações na Europa, Oriente Médio e África. A atuação em solo europeu abre amplas possibilidades de mobilidade aos agentes, devido, porém não limitado, à

União Europeia.

Para combater a criptografia, são realizadas penetrações em redes de empresas de interesse para furtar suas chaves criptográficas, bem como trabalho conjunto com as empresas de tecnologia para secretamente enfraquecer a criptografia utilizada em seus produtos, permitindo a quebra futura.

As agências de inteligência de países desenvolvidos possuem programas de compartilhamento de dados de inteligência, como no caso dos chamados Five Eyes; o programa tendo sido posteriormente estendido para incluir outros parceiros.

O nível tecnológico atual possibilita a criação de sistemas de crédito social, que recompensa comportamento bom e pune comportamento ruim. O estado, sendo o definidor dessa política, decide o que é considerado passível de recompensa ou punição. Por meio do uso de tecnologias de reconhecimento facial, é possível monitorar o trajeto que um indivíduo percorre.

É possível relacionar todas as vezes que ele aparece nas inúmeras câmeras espalhadas por locais públicos e privados, também sendo possível realizar a identificação mesmo depois de alterações no visual, como cortes diferentes de cabelo, barba, ou colocação de acessórios.

O sistema de pontos derivado desse complexo sistema de vigilância pode ser utilizado para refletir quão bom cidadão alguém é. Indivíduos com poucos pontos podem ser punidos com restrições de viagens, maiores impostos, ser impedido de entrar em universidades e ser publicamente humilhado por não ser um bom cidadão. Não há restrições para esse tipo de sistema, prisões ou mortes são teoricamente possíveis. Sendo públicos, os pontos também podem servir de métrica para julgar futuras contratações, amizades e relacionamentos.

Membros familiares também podem ser impactados pelos pontos baixos de seus parentes. Mesmo algo dessa natureza já existindo na China, um sistema de controle dessa magnitude ainda não está em uso no ocidente, contudo, tecnologicamente, não há impedimentos a sua implementação.

O imperialismo americano foi a força criadora (e parte da disseminadora) da internet. Pode-se pensar que a internet apresenta caráter descentralizador, mas esse não é o caso. Na internet moderna, a maior parte do tráfego depende ou passa por um número reduzido de localidades. A internet

moderna é altamente centralizadora. A tecnologia, contudo, pode ser utilizada para a criação de uma rede verdadeiramente descentralizada, mas seria necessária uma reestruturação radical da internet atual, valendo-se de redes federadas e em P2P.

Uma nova fase da internet começou a surgir com a introdução das criptomoedas e de tecnologias blockchain, criadas como resposta para os sistemas bancário e monetário, altamente controlados e manipulados com o intuito de perpetuar o sistema de dominação imposto. Essas soluções, no entanto, comumente falham em verdadeiramente mitigar o problema, como também começam a ser utilizadas para fortalecer o sistema de dominação imposto.

No caso de blockchains, registros inalteráveis sobre as transações dos usuários são fontes valiosas aos donos do poder. A eliminação gradual do dinheiro físico e a introdução de moedas digitais estatais, servem exclusivamente para esse processo. Controle e dominação. Muda-se o contexto, mas o fundamento permanece praticamente inalterado. Tecnologias não são capazes de gerar mudanças em prol da liberdade, caso a mentalidade de seus usuários não seja assim propensa.

A solução não está na tecnologia, mas na tecnologia utilizada como meio de atingir os fins de liberdades estimados pelos indivíduos que a utilizam. Não poderia ser diferente.

Artigo escrito por Gabriel C e revisado por @rodrigo

Tecnologia